AD-A062 537 SYRACUSE UNIV NY DEPT OF ELECTRICAL AND COMPUTER EN--ETC F/G 9/2
WALSH-FUNCTION REPRESENTATION OF SHIFT REGISTERS WITH STOCHASTI--ETC(U)
OCT 78 A U SHANKAR, D K CHENG AFOSR-75-2809

UNCLASSIFIED TR-78-9 AFOSR-TR-78-1631 NL

1 OF 1
AD
A062537

END
DATE
FILMED
3--79
DDC

AD A062537

AFOSR-TR- 78-1631

TR-78-9

LEVEL II

(4)

WALSH-FUNCTION REPRESENTATION OF SHIFT

REGISTERS WITH STOCHASTIC INPUTS

by

A. Udaya Shankar
David K. Cheng

Scientific Report

Grant No. AFOSR-75-2809
Task No. 2304/A3

October 1978

Department of Electrical and Computer Engineering
Syracuse University
Syracuse, New York 13210

78 11 08 039

(12) 13p.

(14) TR-78-9

(11) Oct 78

(4)

(6) WALSH-FUNCTION REPRESENTATION OF SHIFT REGISTERS WITH STOCHASTIC INPUTS.

by

(18) AFOSR

(19) TR-78-1631

(10) A. Udaya/Shankar
David K./Cheng

(9) Scientific Report.

Grant No. AFOSR-75-2809
Task No. 2304/A3

(15) / AFOSR-75-2809

(16) 2304

(17) A3

Approved for public release; distribution unlimited.

October 1978

Department of Electrical and Computer Engineering
Syracuse University
Syracuse, New York 13210

406 737

Table of Contents

Page No.

WALSH-FUNCTION REPRESENTATION OF SHIFT REGISTERS WITH STOCHASTIC INPUTS

A. Udaya Shankar and David K. Cheng
Electrical and Computer Engineering Department, Syracuse University,
Syracuse, New York

ABSTRACT

A Walsh-Hadamard description for the operation of linear-feedback shift registers is presented. It is used to study the transient and steady-state behavior at the outputs of shift registers with respect to a stochastic input and an initial register state.

Introduction

Despite the wide-spread use of linear feedback shift registers (LFSRs), a method for determining the transient and steady-state output statistics of an LFSR in a noisy environment under an initial register state does not appear to be available. In this article we make use of a Walsh-Hadamard representation for the outputs and the external input and characterize the LFSR operation by a set of time-recursive equations over the reals. The equations can be arranged in a matrix form where the matrix involved is sparse and can be written by an inspection of the LFSR. Given a description of the LFSR's initial state and external inputs that are white and stationary, the Walsh-Hadamard representation allows an easy computation of the transient and steady-state output statistics and displays the convergence of the transients in an elegant manner.

Preliminaries

Figure 1 is a schematic of an n-stage LFSR[1], where the feedback coefficients $a_0, a_1, \ldots, a_{n-1}$ are 0 or 1 with a 1 indicating a tap. To ensure a genuine n-stage LFSR we insist that $a_{n-1} = 1$. The feedback at time t is $\overset{n-1}{\underset{k=0}{\textstyle\bigoplus}} a_k y_k(t-1)$, where $\bigoplus$ denotes modulo-2 addition. The transitions of the LFSR are then described by

$$y_o(t) = x(t-1) \oplus \bigoplus_{k=0}^{n-1} a_k y_k(t-1) \tag{1}$$

$$y_k(t) = y_{k-1}(t-1), \quad \text{for} \quad 0 < k < n \tag{2}$$

For any variable, say x, ranging over $\{0,1,\ldots,2^n-1\}$, we denote its binary representation $\langle x_{n-1},\ldots,x_1,x_0\rangle$ by $\bar{x}$. On the domain of the binary n-tuples, the ith Walsh-Hadamard function is defined as[2]

$$\mathrm{Wal}[i,\bar{x}] = (-1)^{\bigoplus_{\ell=0}^{n-1} i_\ell x_\ell} = (-1)^{\sum_{\ell=0}^{n-1} i_\ell x_\ell}, \tag{3}$$

$$\text{for} \quad 0 \le i, \quad x < 2^n$$

where $i = \sum_{\ell=0}^{n-1} i_\ell 2^\ell$ and $x = \sum_{\ell=0}^{n-1} x_\ell 2^\ell$. Because the set of all Walsh functions on the n-tuples form a complete orthogonal basis, any problem on the binary n-tuples can be solved equivalently in the corresponding Walsh domain.

Walsh-Hadamard Description of LFSR

Using the quantities in eqns. 1 and 2 as the exponents of (-1), we obtain, respectively

$$(-1)^{y_o(t)} = (-1)^{x(t-1) \oplus \bigoplus_{k=0}^{n-1} a_k y_k(t-1)} \tag{4}$$

and

$$(-1)^{y_k(t)} = (-1)^{y_{k-1}(t-1)}, \quad \text{for} \quad 0 < k < n \tag{5}$$

In view of eqn. 3, eqns. 4 and 5 become

$$\mathrm{Wal}[2^k, \bar{y}(t)] = \begin{cases} \mathrm{Wal}[1, x(t-1)]\ \mathrm{Wal}[a, \bar{y}(t-1), & \text{for } k = 0 \quad (6) \\ \mathrm{Wal}[2^{k-1}, \bar{y}(t-1)], & \text{for } 0 < k < n \quad (7) \end{cases}$$

where $\bar{y}(t) = \langle y_{n-1}(t), \ldots, y_1(t), y_0(t) \rangle$ and $\bar{a} = \langle a_{n-1}, \ldots, a_1, a_0 \rangle$. We note that eqns. 6 and 7 are insufficient to sustain recursion because $\mathrm{Wal}[a, \bar{y}(t)]$ is not generated.

Now, for every subset of eqns. 6 and 7 a product can be formed to yield a unique equation relating $\bar{y}(t)$ and $\bar{y}(t-1)$. Let $\bar{i}$ for $1 \leq i < 2^n$, indicate by its 1's the equations from eqns. 6 and 7 which are multiplied. Equating the resulting left-hand and right-hand sides, we have

$$\prod_{\ell=0}^{n-1} \{\mathrm{Wal}[2^\ell, \bar{y}(t)]\}^{i_\ell} = \{\mathrm{Wal}[1, x(t-1)]\ \mathrm{Wal}[a, \bar{y}(t-1)]\}^{i_o}$$

$$\times \prod_{\ell=1}^{n-1} \{\mathrm{Wal}[2^{\ell-1}, \bar{y}(t-1)]\}^{i_\ell} \qquad (8)$$

For convenience, we denote $\mathrm{Wal}[i, \bar{y}(t)]$ by $Y_i(t)$ and $\mathrm{Wal}[1, x(t)]$ by $X(t)$. From the property that $\mathrm{Wal}[i, \bar{y}(t)]\ \mathrm{Wal}[j, \bar{y}(t)] = \mathrm{Wal}[i \oplus j, \bar{y}(t)]$, where $\oplus$ is extended to denote dyadic addition (component-wise modulo-2 addition on $\bar{i}$ and $\bar{j}$), eqns. 8 yield

$$Y_i(t) = \begin{cases} X(t-1)\ Y_{(\frac{i-1}{2}) \oplus a}(t-1), & \text{for (odd) } i \in \{1,3,\ldots,2^n-1\} \quad (9) \\ Y_{\frac{i}{2}}(t-1), & \text{for (even) } i \in \{2,4,\ldots,2^n-2\} \quad (10) \end{cases}$$

Eqns. 9 and 10 are capable of sustaining recursion and completely describing the LFSR operation. In fact, denoting the column vector

$[Y_1(t), Y_2(t), \ldots, Y_N(t)]^T$ by $\bar{Y}(t)$, where $N = 2^n - 1$, we can write eqns. 9 and 10 in a matrix form

$$\bar{Y}(t) = \bar{\bar{B}}[X(t-1)]\ \bar{Y}(t-1) \tag{11}$$

where the $N \times N$ matrix $\bar{\bar{B}}[X(t-1)] = \{B_{ij}[X(t-1)]:\ 1 \leq i, j \leq N\}$ has the following elements:

$$B_{ij}[X] = \begin{cases} 1, & \text{for even } i \text{ and } j = i/2 \\ X, & \text{for odd } i \text{ and } j = (\frac{i-1}{2}) \oplus a \\ 0, & \text{otherwise} \end{cases} \tag{12}$$

For $1 \leq i \leq N$: if i is even, then $1 \leq i/2 < 2^{n-1}$; and if i is odd, $2^{n-1} \leq (\frac{i-1}{2}) \oplus a \leq N$ since $a_{n-1} = 1$.

It is clear from eqn. 12 that $\bar{\bar{B}}[X]$, for $X \neq 0$, is a sparse matrix with exactly one nonzero entry in each column and in each row and that the entry is 1 for the first $2^{n-1}-1$ columns and X for the 2^{n-1} succeeding columns. Thus, $\bar{\bar{B}}[X]$ is essentially a *permutation matrix involving the* scaling by X of some elements. For example, a 3-stage LFSR with feedback coefficient vector $\bar{a} = \langle 1\ 0\ 1 \rangle$ will have a 7×7 $\bar{\bar{B}}$-matrix. Since $1 \oplus a = 4$, $2 \oplus a = 7$ and $3 \oplus a = 6$, we have from eqn. 11, using eqn. 12,

$$\begin{bmatrix} Y_1(t) \\ Y_2(t) \\ Y_3(t) \\ Y_4(t) \\ Y_5(t) \\ Y_6(t) \\ Y_7(t) \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 & 0 & X(t-1) & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & X(t-1) & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & X(t-1) \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & X(t-1) & 0 \end{bmatrix} \begin{bmatrix} Y_1(t-1) \\ Y_2(t-1) \\ Y_3(t-1) \\ Y_4(t-1) \\ Y_5(t-1) \\ Y_6(t-1) \\ Y_7(t-1) \end{bmatrix} \tag{13}$$

Returning to eqn. 11, we can express $\bar{Y}(t)$ in terms of its original state, $\bar{Y}(0)$.

$$\bar{Y}(t) = \bar{\bar{B}}[X(t-1)]\ \bar{\bar{B}}[X(t-2)] \ldots \bar{\bar{B}}[X(0)]\ \bar{Y}(0) \tag{14}$$

The product $\bar{\bar{B}}[X(t-1)]\ B[X(t-2)] \ldots \bar{\bar{B}}[X(0)]$ is clearly also a permutation matrix having 1 or -1 as its nonzero entries. When $x(t) \equiv 0$, implying $X(t) \equiv 1$, the LFSR operates as an oscillator with a sequence period which we will denote by p. In this case, $\bar{y}(p) = \bar{y}(0)$ and hence $\bar{\bar{B}}^p[1] = \bar{\bar{I}}$ where $\bar{\bar{I}}$ is the identity matrix of an appropriate dimension.

Output Statistics

We assume a white stationary input so that $x(t_1)$ is independent of but identically distributed as $x(t_2)$ for $t_1 \neq t_2$. This allows the description of the initial state of the LFSR to be independent of the input $x(t)$ for $t \geq 0$. With $E[\cdot]$ denoting expectation, let $\psi_i(t)$ stand for $E[Y_i(t)]$, $\bar{\psi}(t)$ for $E[\bar{Y}(t)]$, and χ for $E[X(t)]$. Then, taking the expectation of eqn. 14 results in the following transient solution.

$$\bar{\psi}(t) = \bar{\bar{B}}^t[\chi]\bar{\psi}(0) \tag{15}$$

The steady-state statistics, if they exist (i.e., if $\bar{\bar{B}}^t[\chi]$ converges), can be found by equating $\bar{\psi}(t)$ to $\bar{\psi}(t-1)$ in the expectation of eqn. 11. We have

$$\bar{\psi}(t)\ (\bar{\bar{I}} - \bar{\bar{B}}[\chi]) = \bar{0} \tag{16}$$

It is seen from eqn. 16 that if $(\bar{\bar{I}} - \bar{\bar{B}}[\chi])^{-1}$ exists, the steady-state $\bar{\psi}(t)$ is uniquely $\bar{0}$. This means that all the outputs are independent and equiprobably 0 or 1. Obviously, for the oscillator case where $\chi = 1$ or -1, a steady-state statistic does not exist except for the trivial case of $\bar{\psi}(0) = \bar{0}$. Thus, $(\bar{\bar{I}} - \bar{\bar{B}}[1])^{-1}$ and $(\bar{\bar{I}} - \bar{\bar{B}}[-1])^{-1}$ do not exist.

The eigenvalues of $\bar{\bar{B}}[\chi]$ control the time convergence of the LFSR output statistics. Indeed, denoting the N eigenvalues of $\bar{\bar{B}}[\chi]$ by $\lambda_1, \lambda_2, \ldots, \lambda_N$, some of which may be equal, we may write

$$\bar{\bar{B}}^t[\chi] = \lambda_1^t \, \bar{\bar{C}}(1) + \lambda_2^t \, \bar{\bar{C}}(2) + \ldots + \lambda_N^t \, \bar{\bar{C}}(N) \tag{17}$$

where the matrices $\bar{\bar{C}}(1), \bar{\bar{C}}(2), \ldots, \bar{\bar{C}}(N)$ are determined from the eigenvectors. As $t \to \infty$, an eigenvalue of a magnitude greater than 1 would cause $\bar{\bar{B}}^t[\chi]$ and hence $\bar{\psi}(t)$ to explode, which is not allowed physically. Thus $|\lambda_i| \leq 1$ for $1 \leq i \leq N$. If the magnitude of an eigenvalue is 1, eqns. 15 and 17 indicate that, at steady state, $\bar{\psi}(t)$ would be a non-decaying periodic function. In view of the constantly growing uncertainty introduced by $x(t)$, such a $\bar{\psi}(t)$ is possible if and only if $\chi \in \{1, -1\}$. This implies determinism right from the outset. Thus, if $|\chi| < 1$, we expect the contents of LFSR to ultimately reach maximum entropy; i.e., $\bar{\psi}(t) \equiv 0$.

The above observations may be summarized as follows: (i) $|\lambda_i| \leq 1$ for all $1 \leq i < N$; (ii) $|\chi| = 1$ if and only if $|\lambda_i| \in \{1,0\}$ for any $1 \leq i < N$ with at least one eigenvalue having a unit magnitude; and (iii) $|\chi| < 1$ if and only if $|\lambda_i| < 1$ for all $1 \leq i < N$. From eqn. 17, if λ_m is the eigenvalue of the greatest magnitude and $|\chi| < 1$, then the entries in $\bar{\bar{B}}^t[\chi]$ will decay to zero at least as fast as $|\lambda_m|^t$.

The joint probability distribution of $\bar{y}(t)$ can be obtained from $\bar{\psi}(t)$ via the Walsh-transform relationship. By definition,

$$\psi_i(t) = \sum_{\ell=0}^{N} \Pr[\bar{y}(t) = \bar{\ell}] \, \mathrm{Wal}[i,\bar{\ell}] \tag{18}$$

The inverse transformation of eqn. 18 is

$$\Pr[\bar{y}(t) = \bar{\mu}] = 2^{-n}[1 + \sum_{i=1}^{N} \psi_i(t)\ \mathrm{Wal}[i, \bar{\mu}]] \tag{19}$$

We may conclude that, for $|\chi| < 1$, $\psi_i(t)$ converges to 0 and $\Pr[\bar{y}(t) = \bar{\mu}]$ converges to 2^{-n}, also at least as fast as $|\lambda_m|^t$.

For the example considered in eqn. 13 the output statistic $\gamma(t) = \Pr[\bar{y}(t)=\langle 001\rangle]$ is plotted versus t in Fig. 2 for an initial state <001> for two values of χ. For this maximum-length 3-stage LFSR (p=7), $\lambda_i = \chi^{4/7} \exp(2\pi i\sqrt{-1}/7)$, i = 1,2,...,7. Thus, $|\lambda_i| = \chi^{4/7}$. We observe from Fig. 2 that (i) $\gamma(t) = 0$ for t = 1 and t = 2 irrespective of x(t) for the given initial state <0 0 1>, as expected, (ii) $\gamma(t)$ converges to 2^{-3} = 0.125, as predicted by eqn. 19; and (iii) $|\gamma(t+7) - 2^{-3}| / |\gamma(t) - 2^{-3}| = \chi^4$ — Convergence is faster for a smaller χ.

Conclusion

The behaviour of linear-feedback shift registers is neatly captured by a Walsh-Hadamard representation in the form of a matrix recursive equation which can be written by inspection and which yields the output statistics for a stochastic input quite easily. Because the representation is over the reals where our intuition is stronger, it facilitates our study of the transient and convergence properties in terms of the eigenvalues of a permutation matrix.

References

1. GOLOMB, S. W.: 'Shift register sequences' (Holden-Day, San Francisco. 1967), chap. 3, pp. 24-35.

2. KREMER, H.: "Representation and mutual relations of the different systems of Walsh functions," Colloq. on Theory and Applications of Walsh Functions, Hatfield Polytechnic, Herts., U.K., June 28-29, 1973.

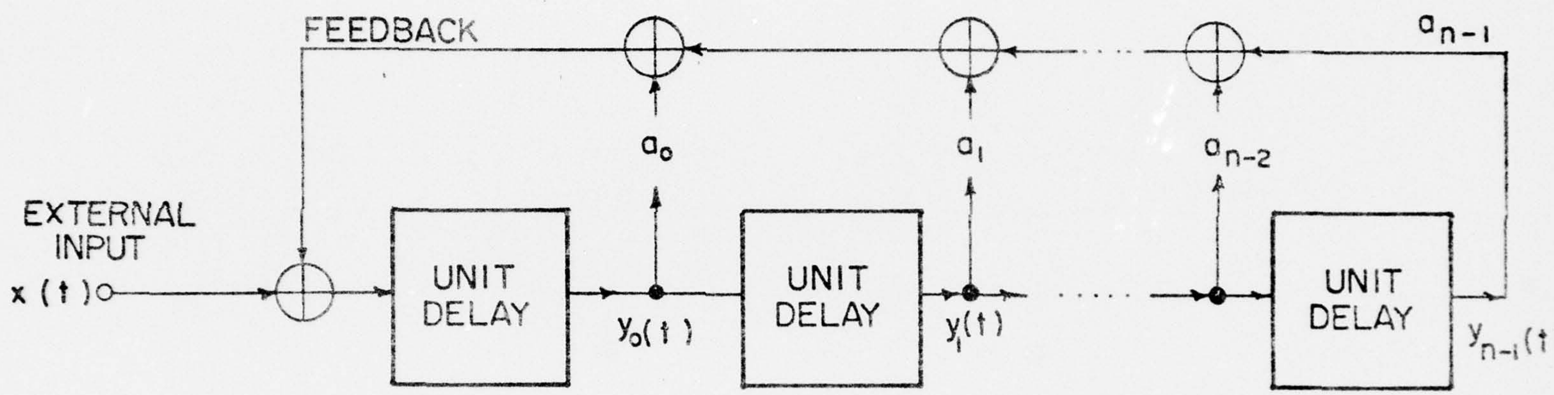

Fig. 1 - Schematic of an n-stage LFSR.

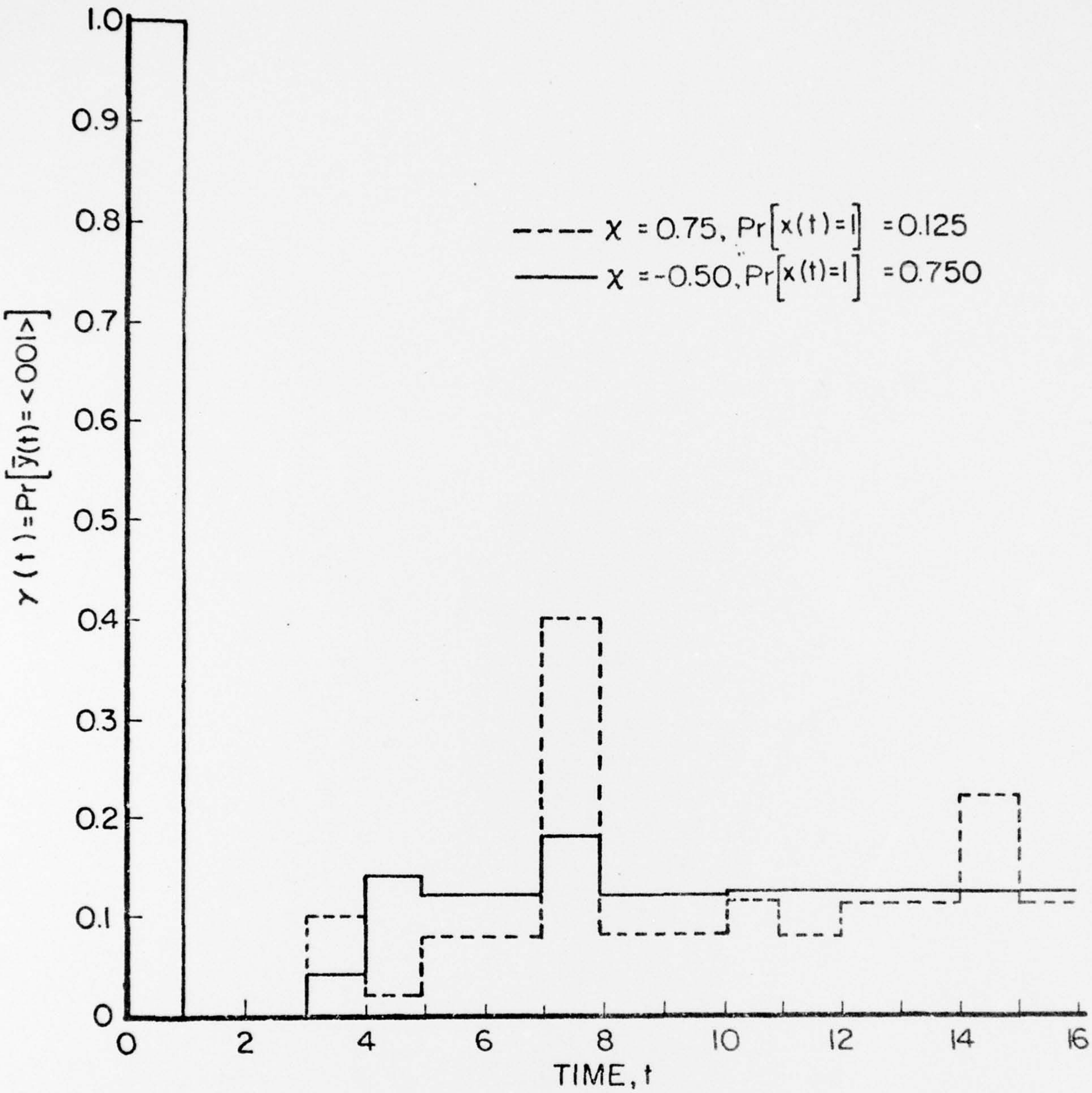

Fig. 2 - Output probability of a 3-stage maximum-length LFSR versus time: $\bar{a} = \langle 1\ 0\ 1 \rangle$, $\bar{y}(0) = \bar{\mu} = \langle 0\ 0\ 1 \rangle$.

REPORT DOCUMENTATION PAGE		READ INSTRUCTIONS BEFORE COMPLETING FORM
1. REPORT NUMBER AFOSR-TR- 78-1631	2. GOVT ACCESSION NO.	3. RECIPIENT'S CATALOG NUMBER
4. TITLE (and Subtitle) WALSH-FUNCTION REPRESENTATION OF SHIFT REGISTERS WITH STOCHASTIC INPUTS		5. TYPE OF REPORT & PERIOD COVERED Interim
		6. PERFORMING ORG. REPORT NUMBER TR-78-9
7. AUTHOR(s) A. Udaya Shankar and David K. Cheng		8. CONTRACT OR GRANT NUMBER(s) AFOSR 75-2809
9. PERFORMING ORGANIZATION NAME AND ADDRESS Syracuse University Dept. of Elec. and Computer Eng. Syracuse, New York 13210		10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS 61102F 2304/A3
11. CONTROLLING OFFICE NAME AND ADDRESS Air Force Office of Scientific Research/NM Bolling AFB, Washington, DC 20332		12. REPORT DATE October 1978
		13. NUMBER OF PAGES 11
14. MONITORING AGENCY NAME & ADDRESS(if different from Controlling Office)		15. SECURITY CLASS. (of this report) UNCLASSIFIED
		15a. DECLASSIFICATION/DOWNGRADING SCHEDULE

16. DISTRIBUTION STATEMENT (of this Report)

Approved for public release; distribution unlimited.

17. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, if different from Report)

18. SUPPLEMENTARY NOTES

19. KEY WORDS (Continue on reverse side if necessary and identify by block number)

20. ABSTRACT (Continue on reverse side if necessary and identify by block number)

A Walsh-Hadamard description for the operation of linear-feedback shift registers is presented. It is used to study the transient and steady-state beharior at the outputs of shift registers with respect tc a stochastic input and an initial register state.

DD FORM 1 JAN 73 1473